بسم الله الرحمن الرحيم

والصلاة والسلام على اشرف المرسلين

سيدنا محمد وعلى الة وصحبة اجمعين

كتاب ال **ISecP**

امن برتكول IP

اعداد:

محمد الطيب محمد

mtma50@gmail.com

مقدمة:

- ما هي ال IPSec؟

IPSec: هي مجموعة معايير من البروتوكولات والخوارزميات طورت بواسطة اللجنة الخاصة لنظام الإنترنت Internet Engineering Task Force (IETF) واعتمدت كمعايير الإنترنتِ لتوفر التحقق من سلامة وسرية المعلومات التي أرسلت عبر شبكات الIP، وذلك بجعلها تعمل في طبقة الIP بحيث تتمكن من حماية أي نوع من نقل البيانات من خلال الIP.

عادةً يعبر عن الIPSec بأنها Transparent Security Protocol لأن المستخدم و التطبيقات لايشعرون بوجودها لأنها تعمل على طبقة الشبكة (Network Layer)، ويعمل ال IPSecفي البيئات التي تكون سرعة الاتصال بها سريعة.

- بروتوكولات الIPSec

ينقسم ال IPSecالى ثلاث بروتوكولات:

<u>أولاً: AH : Authentication Header</u>

يستخدم الAH في توقيع Sign الرسائل والبيانات ولا يعمل على تشفيرها Encryption ، حيث يحافظ على:

١.موثوقية البيانات **Data authenticity:**
أي أن البيانات المرسلة من هذا
المستخدم هي منه وليست مزورة أو
مدسوسة.

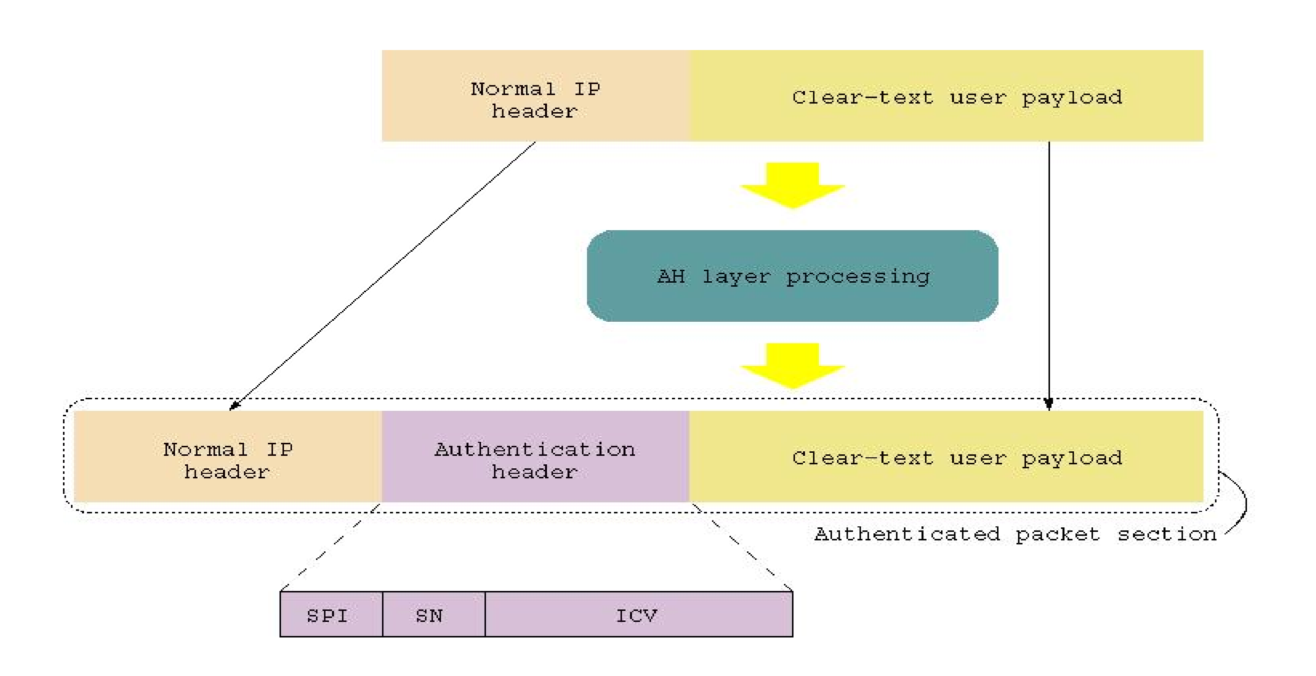
٢.صحة البيانات **Data Integrity** : أي أن
البيانات المرسلة لم يتم تعديلها على
الطريق (أثناء مرورها على الأسلاك) .

٣.عدم إعادة الإرسال **Anti-Replay** :
وهذه الطريقة التي يستخدمها المخترقون
حيث يقومون بسرقة كلمة المرور وهي
مشفرة ويقومون بإعادة إرسالها في وقت
آخر للسيرفر وهي مشفرة وبالطبع يفك
السيرفر التشفير ويدخل اسم المستخدم
على أنه شخص آخر، فالIPSec يقدم حلولاً
لمنع هذه العملية من الحدوث.

٤.الحماية ضد الخداع **Anti-Spoofing**
protection : ويوفر أيضاً الIPSec حماية
ضد الخداع من قبل المستخدمين ، مثلاً
يمكن ان يحدد مدير الشبكه انه لا يسمح
لغير المستخدمين على ال subnet
192.168.0.X بينما لا يسمح لحاملي

الهويه ١٩٢.١٦٨.١.x من دخول السيرفر ، فيمكن للمستخدم ان يغير الIP Address الخاص به ، لكن الIPSec يمنع ذلك .(وايضا يمكنك القياس على ذلك من خارج الشبكه الى داخلها) يكون لكل حزمة Packet موقعها Digitally signed.

هذا هو الشكل العام لحزمة البيانات Packet التي تمر في بروتوكول AH .



<u>ثانياً: ESP : Encapsulating Security Payload</u>

يوفر هذا البروتوكول التشفير والتوقيع للبيانات معا Encryption and Signing ، و يستخدم هذا البروتوكول في كون

المعلومات سرية Confidential او Secret ، أو عند إرسال المعلومات عن طريق Public Network مثل الانترنت.
يوفر الESP المزايا التالية:

١.**Source authentication** : وهي مصداقية المرسل ، حيث كما وضحنا في مثال الSpoofing أنه لا يمكن لأي شخص يستخدم الIPSec تزوير هويته (هوية المرسل).

٢.التشفير للبيانات **Data Encryption** : حبث يوفر التشفير للبيانات لحمايتها من التعديل أو التغيير أو القراءة.

٣.**Anti-Replay** : موضحة في الAH .

٤.**Anti-Spoofing Protection** : موضحة في ال AH.

<u>ثالثاً : Internet Key Exchange : IKE</u>

الوظيفة الاساسيه لهذا البروتوكول هي ضمان الكيفية وعملية توزيع ومشاركة المفاتيح Keys بين مستخدمي الIPSec ،

فهو بروتوكول الnegotiation أي النقاش في نظام الIPSec كما أنه يعمل على تأكيد طريقة الموثوقية Authentication والمفاتيح الواجب استخدامها ونوعها (حيث ان الIPSec يستخدم التشفير DES٣ وهو عبارة عن زوج من المفاتيح ذاتها يتولد عشوائياً بطرق حسابية معقدة ويتم إعطاءه فقط للجهة الثانية ويمنع توزيعه وهو من نوع Symmetric Encryption أي التشفير المتوازي ويستخدم تقنية الPrivate Key .

- أقسام الIPSec

أو انواع الIPSec التي يستخدمها في الشبكة، وينقسم الIPSec الى نظامين او نوعين وهما :

١. نظام النقل Transport Mode

٢. نظام النفق Mode Tunnel .

نظام النقل: يستخدم هذا النظام عادة داخل الشبكة المحلية LAN : Local Area Network حبث يقدم خدمات التشفير للبيانات التي تتطابق والسياسة المتبعة في الIPSec بين أي جهازين في الشبكه

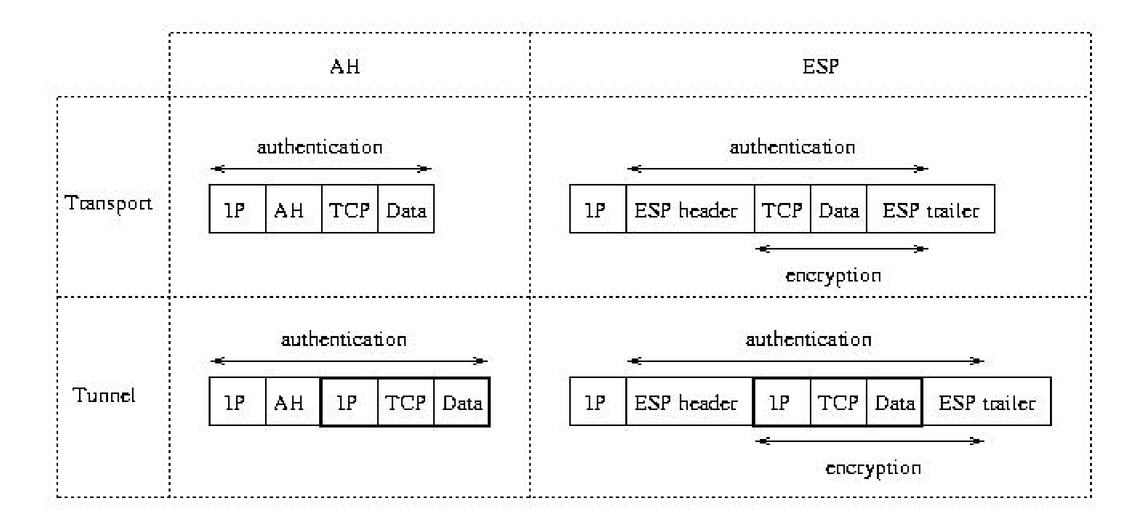
أي يوفر Endpoint-to-Endpoint Encryption فمثلاً اذا قمت بضبط سياسة الـIPSec على تشفير جميع الحركة التي تتم على بورت ٢٣ وهو بورت الـTelnet (حيث ان الـTelnet ترسل كل شيء مثلما هو دون تشفير Text Plain) فإذا تمت محادثه بين السيرفر والمستخدم على هذا البورت فان الـIPSec يقوم بتشفير كل البيانات المرسلة من لحظت خروجها من جهاز المستخدم الى لحظة وصولها الى السيرفر. يتم تطبيق هذا النظام في الحالات التالية:

أولاً: المحادثة تتم بين الأجهزة في داخل أو نفس الشبكة الداخلية الخاصة Private LAN.

ثانياً: المحادثة تتم بين جهازين ولا يقطع بينهما Firewall حائط ناري يعمل عمل NAT (نظام : Network Address Translation يمكن الـFirewall من استبدال جميع عناوين الـIPs في الشبكه الداخليه من حزمة البيانات Packet واستبدالها في عنوان Public IP اخر ، ونستفيد من ذلك

هو أننا لن نحتاج سوى الى عنوان IP واحد One Public IP ، وأيضاً أنه يقوم بإخفاء عناوين الأجهزه عن شبكة الانترنت للحماية من الاختراق الخارجي) .
نظام النفق: يتم استخدام هذا النظام لتطبيق الـIPSec بين نقطتين تكون بالعادة بين ٢ Routers ، إذاً يتم استخدام هذا النظام بين نقطتين بعيدتين جغرافياً أي سيتم قطع الانترنت في طريقها الى الطرف الثاني ، مثل الاتصالات التي تحدث بين الشبكات المتباعده جغرافيا WAN : Wide Network Area ، يستخدم هذا النظام فقط عند الحاجه لتأمين البيانات فقط اثناء مرورها من مناطق غير آمنة كالانترنت ، فمثلاً إذا أراد فرعين لشركة أن يقوم بتشفير جميع البيانات التي يتم إرسالها فيما بينهم على بروتوكول FTP : File Transfer Protocol فيتم إعداد الـIPSec على أساس الـTunnelling Mode .

وهذه صوره مخطط لكل من الـPackets في الـAH ، ESP في كلتا النظامين Tunnel and Transport Modes .



- فوائده IPSec Benefits

لقد ظهر ضعف كبير في عملية الEncryption العادية التي تتم بين الأجهزه في الشبكات ، وهذا الضعف تمثل في صعوبة تطبيق هذا الموضوع ، وأيضا استهلاكه للوقت أي بطؤه الشديد في القيام بعملية التشفير وفكه Encryption and decryption،فالفائدة الكبرى التي ظهرت في الIPSec هي أنه يوفر حماية كاملة وواضحة لجميع البروتوكولات التي تعمل على الطبقة الثالث Layer 3 of the OSI Model وما بعدها.

من مميزات الIPSec أيضا هو أنه موجود

أصلاً Built-in في داخل حزمة الIP Packet ، فلذلك هو لا يحتاج لأي إعدادت لانتقاله عبر الشبكة ولا يحتاج لأي أجهزة إضافية لذلك .

- كيف يحمي الIPSec من الهجوم على الشبكة؟

إن الشبكة والبيانات التي تمر فيها يمكن ان تتعرض للعديد من أنواع الهجمات المختلفة ، بعض الهجمات تكون غير فعاله Passive مثل مراقبة الشبكة Network Monitoring ، ومنها ما هو الفعال Active مما يعني أنها يمكن أن تتغير البيانات أو تسرق في طريقها عبر أسلاك الشبكة. و سوف نستعرض بعض انواع الهجمات على الشبكات.

أولاً: التقاط حزم البيانات Eavesdropping, sniffing or snooping:حيث يتم بذلك مراقبة حزم البيانات التي تمر على الشبكه بنصها الواضح دون تشفير Plain text والتقاط ما نريد منها ، ويعالجها الIPSec عن طريق

تشفير حزمة البيانات، عندها حتى لو التقطت الحزمة فإن الفاعل لن يستطيع قراءتها أو العبث بها، لأن الطرف الوحيد الذي يملك مفتاح فك التشفير هو الطرف المستقبل.

ثانيا: تعديل البيانات Data modification:حيث يتم بذلك سرقة حزم البيانات من الشبكة ثم تعديلها وإعادة إرسالها إلى المستقبل، ويقوم الIPSec بمنع ذلك عن طريق استخدام الهاش Hash ووضعه مع البيانات ثم تشفيرها معاً ، وعندما تصل الحزمة إلى الطرف المستقبل فإن الجهاز يفحص Checksum التابع للحزمة إذا تمت مطابقته أم لا، فإذا تمت المطابقة مع الهاش الأصلي المشفر تبين أن الحزمة لم تعدل، لكن إذا تغير الهاش فإن حزمة البيانات قد تم تغييرها على الطريق.

ثالثاً: انتحال الشخصية Identity spoofing: بحيث يتم استخدام حزم البيانات على الشبكة والتقاطها وتعديلها لتبين هوية مزورة للمرسل، أي خداع المستقبل بهوية المرسل، ويمنع ذلك عن طريق الطرق الثلاثه التي يستخدمها الIPSec وهي: بروتوكول الكيربرس

(Protocol Kerberos)، والشهادات الالكترونية Digital Certificates، ومشاركة مفتاح معين (Preshared Key).
حيث لا تتم عملية بدأ المحادثة وإرسال البيانات قبل التأكد من صحة الطرف الثاني عن طريق احدى الطرق المذكورة.

رابعاً: Service DoS -Denial of رفض الخدمة أو حجبها: حيث تعمل هذه الهجمة على تعطيل خدمة من خدمات الشبكه للمستخدمين والمستفيدين منها ، مثلاً كاشغال السيرفر في الشبكة بعمل عليه Flood مما يشغله بالرد على هذه الأمور وعدم الاستجابة للمستخدمين.
ويعمل الـIPSec على منع ذلك عن طريق إمكانية غلقه أو وضع قواعد للمنافذ المفتوحة Ports.
خامساً: Middle MITM -Man In The:
من أشهر الهجمات في الشبكات، وهي أن يكون هنالك طرف ثالث يعمل على سرقة البيانات المرسلة من طرف لآخر وإمكانية العمل على تعديلها أو العمل على عدم إيصالها للجانب الاخر، ويعمل الـIPSec على منعه بواسطة طرق التحقق من الموثوقية

. Authentication methods

سادساً: الهجمات على طبقة التطبيقات Application Layer Attacks : حيث تعمل هذه الهجمات على التأثير على النظام المستخدم في أجهزة الشبكة وأيضاً تعمل على التأثير على البرامج المستخدمة في الشبكة، ومن الأمثله عليها الفيروسات والديدان التي تنتشر بفعل ثغرات في الأنظمة أو البرامج أو حتى اخطاء المستخدمين. يعمل الIPSec على الحماية من ذلك بكونه يعمل على طبقة IP Layer فيعمل على إسقاط أي حزمة بيانات لا تتطابق مع الشروط الموضوعة لذلك ، لذا فتعمل الفلاتر على إسقاطها وعدم إيصالها للأنظمة أو البرامج.

بشكل عام فالIPSec يحمي من معظم الهجمات عن طريق استخدامه ميكانيكية التشفير المعقدة ، حيث يوفر التشفير الحماية للبيانات والمعلومات ايا كانت اثناء انتقالها على الوسط (اياً كان) عن طريق عمليتي التشفير Encryption والهاش Hashing.

طريقة التشفير المستخدمة في الIPSec عبارة عن دمج لعدة Algorithms ومفاتيح، وحيث
Algorithm: عباره عن العملية الحسابية التي تمر فيها البيانات لكي تشفر.
Key: وهو عباره عن رقم (كود) سري يتم من خلاله قراءه أو تعديل أو حذف أو التحكم في البيانات المشفرة بشرط مطابقته للطرف الثاني الذي قام بعملية التشفير.

